U.S. Department of Justice

Federal Bureau of Investigation
Washington, D.C. 20535

April 14, 2015

MS. ALEXA O'BRIEN
[redacted]

FOIPA Request No.: 1324716-000
Subject: LULZSEC

Dear Ms. O'Brien:

Records responsive to your request were previously processed under the provisions of the Freedom of Information Act. Enclosed is one CD containing 63 pages of previously-processed documents and a copy of the Explanation of Exemptions. Documents or information originating with other Government agencies originally referred to that agency were not included in this release. This release is being provided to you at no charge.

Additional records potentially responsive to your subject may exist. Please submit a new FOIA request if you would like the FBI to conduct a search of the indices to our Central Records System.

Submit requests by mail or fax to – Initial Processing, 170 Marcel Drive, Winchester, VA 22602, fax number (540) 868-4997.

For your information, Congress excluded three discrete categories of law enforcement and national security records from the requirements of the FOIA. See 5 U.S. C. § 552(c) (2006 & Supp. IV (2010). This response is limited to those records that are subject to the requirements of the FOIA. This is a standard notification that is given to all our requesters and should not be taken as an indication that excluded records do, or do not, exist.

You may file an appeal by writing to the Director, Office of Information Policy (OIP), U.S. Department of Justice, 1425 New York Ave., NW, Suite 11050, Washington, D.C. 20530-0001, or you may submit an appeal through OIP's eFOIA portal at http://www.justice.gov/oip/efoia-portal.html. Your appeal must be received by OIP within sixty (60) days from the date of this letter in order to be considered timely. The envelope and the letter should be clearly marked "Freedom of Information Appeal." Please cite the FOIPA Request Number assigned to your request so that it may be identified easily.

Sincerely yours,

David M. Hardy
Section Chief,
Record/Information
Dissemination Section
Records Management Division

Enclosure(s)

EXPLANATION OF EXEMPTIONS

SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552

(b)(1) (A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified to such Executive order;

(b)(2) related solely to the internal personnel rules and practices of an agency;

(b)(3) specifically exempted from disclosure by statute (other than section 552b of this title), provided that such statute (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld;

(b)(4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;

(b)(5) inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;

(b)(6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;

(b)(7) records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information (A) could reasonably be expected to interfere with enforcement proceedings, (B) would deprive a person of a right to a fair trial or an impartial adjudication, (C) could reasonably be expected to constitute an unwarranted invasion of personal privacy, (D) could reasonably be expected to disclose the identity of confidential source, including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of record or information compiled by a criminal law enforcement authority in the course of a criminal investigation, or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source, (E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or (F) could reasonably be expected to endanger the life or physical safety of any individual;

(b)(8) contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions; or

(b)(9) geological and geophysical information and data, including maps, concerning wells.

SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552a

(d)(5) information compiled in reasonable anticipation of a civil action proceeding;

(j)(2) material reporting investigative efforts pertaining to the enforcement of criminal law including efforts to prevent, control, or reduce crime or apprehend criminals;

(k)(1) information which is currently and properly classified pursuant to an Executive order in the interest of the national defense or foreign policy, for example, information involving intelligence sources or methods;

(k)(2) investigatory material compiled for law enforcement purposes, other than criminal, which did not result in loss of a right, benefit or privilege under Federal programs, or which would identify a source who furnished information pursuant to a promise that his/her identity would be held in confidence;

(k)(3) material maintained in connection with providing protective services to the President of the United States or any other individual pursuant to the authority of Title 18, United States Code, Section 3056;

(k)(4) required by statute to be maintained and used solely as statistical records;

(k)(5) investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment or for access to classified information, the disclosure of which would reveal the identity of the person who furnished information pursuant to a promise that his/her identity would be held in confidence;

(k)(6) testing or examination material used to determine individual qualifications for appointment or promotion in Federal Government service he release of which would compromise the testing or examination process;

(k)(7) material used to determine potential for promotion in the armed services, the disclosure of which would reveal the identity of the person who furnished the material pursuant to a promise that his/her identity would be held in confidence. FBI/DOJ

FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1324716-0

Total Deleted Page(s) = 6
Page 8 ~ b6; b7C; b7D;
Page 9 ~ b6; b7C; b7D;
Page 12 ~ b6; b7C; b7D;
Page 19 ~ b6; b7C; b7D;
Page 20 ~ b7D;
Page 21 ~ b7D;

XXXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXXXXX

(Rev. 05-01-2008)

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 10/03/2011

To: Albany

From: Albany
[redacted]
Contact: SA [redacted]

b6
b7C

Approved By: [redacted] PDS

Drafted By: [redacted]:dia DA

Case ID #: 288A-AL-~~NEW~~ 49289 (Pending) - 1

Title: ANONYMOUS - HACKTIVISTS;
LULZSEC - HACKTIVISTS;
BACKTRACE SECURITY - HACKTIVISTS;
ET AL - HACKTIVISTS;
COMPUTER INTRUSIONS

Synopsis: [redacted]
NTP-014
CRINT-C

OTA PDS 10/4/11

b7E

Full Investigation Initiated: 10/03/2011

Details: The Albany division is opening [redacted] to investigate the activities of the captioned hacker groups. Albany has recently opened a CHS who is in a position to provide significant intelligence on the captioned groups.

b7E

By way of background, Anonymous is a hacktivist group that originated in 2003 on the 4chan imageboard. In its early days, Anonymous members were a largely decentralized online group acting in a loosely coordinated manner. Starting in 2008, the group became associated with international hacktivism and has claimed responsibility for several computer intrusions and Distributed Denial of Service (DDoS) attacks. Some of the more well known victims of attacks attributed to Anonymous include Sony, Church of Scientology, and HBGary Federal.

b6
b7C

By way of background, Lulz Security (LulzSec) is a hacktivist group that has claimed responsibility for several

OTA [redacted] 10/4/11 DG

UNCLASSIFIED

288A-AL-49289-1

273dia03.ec.wpd

computer intrusions and incidents of "doxing". "Doxing" is the practice of releasing personal and confidential information about persons and organizations including contact information, biographical information, usernames, passwords, and other sensitive data. Some of LulzSec's targets have included Sony and various government and law enforcement organizations.

In June 2011, Albany executed arrest and search warrants on an identified LulzSec member [redacted]. This individual was residing in Albany's AOR and was actively participating in high profile intrusion activity attributed to LulzSec. b7A

By way of background, BackTrace Security is a hacker group that spun off of Anonymous because they disagree with the current direction that Anonymous has taken. Backtrace Security does not believe in the political hacktivism activities that Anonymous has claimed responsibility for lately. One of the goals of Backtrace Security is to put an end to the current incarnation of Anonymous. Backtrace Security has also attempted to identify members of LulzSec and shut down their operations.

[redacted] has agreed to work with the writer [redacted] b7D

[redacted] is the second Albany CHS to be opened in the past year that has verified ties to identified hacker groups responsible for criminal computer intrusion activity. [redacted] as deemed appropriate by the case agent.

It is requested that a case be opened and assigned to SA [redacted] b6 b7C

♦♦

UNCLASSIFIED

FD-1023 (07/24/2010)	FEDERAL BUREAU OF INVESTIGATION CHS REPORTING DOCUMENT

HEADER

Source ID:

Date: **10/07/2011**

Case Agent Name:

Field Office/Division: **Albany**

Squad:

b6
b7C
b7D

Date of Contact: **10/05/2011**

List all present including yourself. (Do not include the CHS.): SA

Type of Contact: **e-Mail**

Date of Report: **10/05/2011**

Substantive Case File Number: **288A-AL-49289** 2

Substantive Case File Number: **803I-AL-48481**

Source Reporting: The following information was provided via email by CHS between 09/20/2011 and 10/05/2011. The information was volunteered by CHS. It was not the result of a tasking. The information was not specifically requested by the handling agent. The information was provided on a confidential basis prior to the admonishment of CHS:

b7D

288A-AL-49289-2

b7D

Signed by:

Click here to sign this section

Signed by [redacted] View details
on Friday, October 07, 2011 5:20 PM (Eastern Daylight Time)

b6
b7C

Signed by [redacted] View details
on Tuesday, October 11, 2011 3:36 PM (Eastern Daylight Time)

FD-1023 (07/24/2010)	FEDERAL BUREAU OF INVESTIGATION

UNCLASSIFIED

FD-1023 (07/24/2010)	FEDERAL BUREAU OF INVESTIGATION CHS REPORTING DOCUMENT

HEADER

Source ID:

Date: **10/07/2011**

Case Agent Name:

Field Office/Division: **Albany**

Squad:

Date of Contact: **09/22/2011**

List all present including yourself. (Do not include the CHS.): SA

SA

Type of Contact: **In Person**

Country: **UNITED STATES**

City:

State:

Date of Report: **09/22/2011**

Substantive Case File Number: **288A-AL-49289** -3

Source Reporting: On 09/22/2011, after being advised of the identity of the interviewing agents and the nature of the interview, CHS provided the following:

b6
b7C
b7D

b7D

288A-AL-49289
-3

Signed by [redacted] View details
on Tuesday, October 11, 2011 3:46 PM (Eastern Daylight Time)

b6
b7C

FD-1023 (07/24/2010)	FEDERAL BUREAU OF INVESTIGATION

UNCLASSIFIED

FD-1023 (07/24/2010)	FEDERAL BUREAU OF INVESTIGATION CHS REPORTING DOCUMENT

HEADER

Source ID:

Date: **10/07/2011**

Case Agent Name:

Field Office/Division: **Albany**

Squad:

b6
b7C
b7D

Date of Contact: **09/29/2011**

List all present including yourself. (Do not include the CHS.): SA

Type of Contact: **In Person**

Country: **UNITED STATES**

City:

State:

Date of Report: **09/29/2011**

b6
b7C

Substantive Case File Number: **288A-AL-49289** -4

Source Reporting: On 09/29/2011, SA met with CHS at his home. After being advised of the identity of the interviewing agent and the nature of the interview, CHS provided the following:

b6
b7C
b7D

288A-AL-49289-4

Click here to sign this section

Signed by [redacted] View details
on Friday, October 07, 2011 3:58 PM (Eastern Daylight Time)

Signed by [redacted] View details
on Tuesday, October 11, 2011 3:48 PM (Eastern Daylight Time)

b6
b7C

FD-1023 (07/24/2010)	FEDERAL BUREAU OF INVESTIGATION

UNCLASSIFIED

FD-1023 (07/24/2010)	FEDERAL BUREAU OF INVESTIGATION CHS REPORTING DOCUMENT

HEADER

Source ID:

Date: **10/07/2011**

Case Agent Name:

Field Office/Division: **Albany**

Squad:

Date of Contact: **10/06/2011**

List all present including yourself. (Do not include the CHS.): SA

b6
b7C
b7D

Type of Contact: **In Person**

Country: **UNITED STATES**

City:

State

Date of Report: **10/06/2011**

Substantive Case File Number: **288A-AL-49289** -5

Source Reporting: On 10/06/2011, after being advised of the identity of the interviewing agent and the nature of the interview, CHS provided the following:

b6
b7C
b7D

Signed by:

Click here to sign this section

288A-AL-49289
-5

Signed by [redacted] View details
on Friday, October 07, 2011 3:59 PM (Eastern Daylight Time)

Signed by [redacted] View details
on Tuesday, October 11, 2011 3:49 PM (Eastern Daylight Time)

b6
b7C

FD-1023 (07/24/2010)	FEDERAL BUREAU OF INVESTIGATION

UNCLASSIFIED

FD-1023 (07/24/2010)	FEDERAL BUREAU OF INVESTIGATION CHS REPORTING DOCUMENT

HEADER

Source ID:

Date: **11/07/2011**

Case Agent Name:

Field Office/Division: **Albany**

Squad:

Date of Contact: **11/04/2011**.

List all present including yourself. (Do not include the CHS.): SA

Type of Contact: **In Person**

Country: **UNITED STATES**

City

State

Date of Report: **11/04/2011**

Substantive Case File Number: **288A-AL-49289** -6

Source Reporting: On 11/04/2011, CHS provided the following:

Signed by:

Click here to sign this section

Signed by View details
on Monday, November 07, 2011 11:20 AM (Eastern Daylight Time)

Signed by View details
on Monday, November 07, 2011 11:30 AM (Eastern Daylight Time)

288A-AL-49289-6

UNCLASSIFIED

FD-1023 (07/24/2010)	FEDERAL BUREAU OF INVESTIGATION CHS REPORTING DOCUMENT

HEADER

Source ID:

Date: **02/08/2012**

Case Agent Name:

Field Office/Division: **Albany**

Squad:

Date of Contact: **02/07/2012**

List all present including yourself. (Do not include the CHS.): SA

b6
b7C
b7D

Type of Contact: **In Person**

Country: **UNITED STATES**

City:

State:

Date of Report: **02/07/2012**

Substantive Case File Number: **288A-AL-49289** -7

Source Reporting: On 02/07/2012, CHS provided the following:

b6
b7C
b7D

Signed by:

Click here to sign this section

Signed by View details
on Wednesday, February 08, 2012 10:10 AM (Eastern Daylight Time)

b6
b7C

Signed by View details
on Thursday, February 09, 2012 4:08 PM (Eastern Daylight Time)

288A-AL-49289-7

UNCLASSIFIED

FD-1023 (07/24/2010)	FEDERAL BUREAU OF INVESTIGATION CHS REPORTING DOCUMENT

HEADER

Source ID:

Date: **11/28/2011**

Case Agent Name:

Field Office/Division: **Albany**

Squad:

b6
b7C
b7D

Date of Contact: **11/24/2011**

List all present including yourself. (Do not include the CHS.): SA

Type of Contact: **e-Mail**

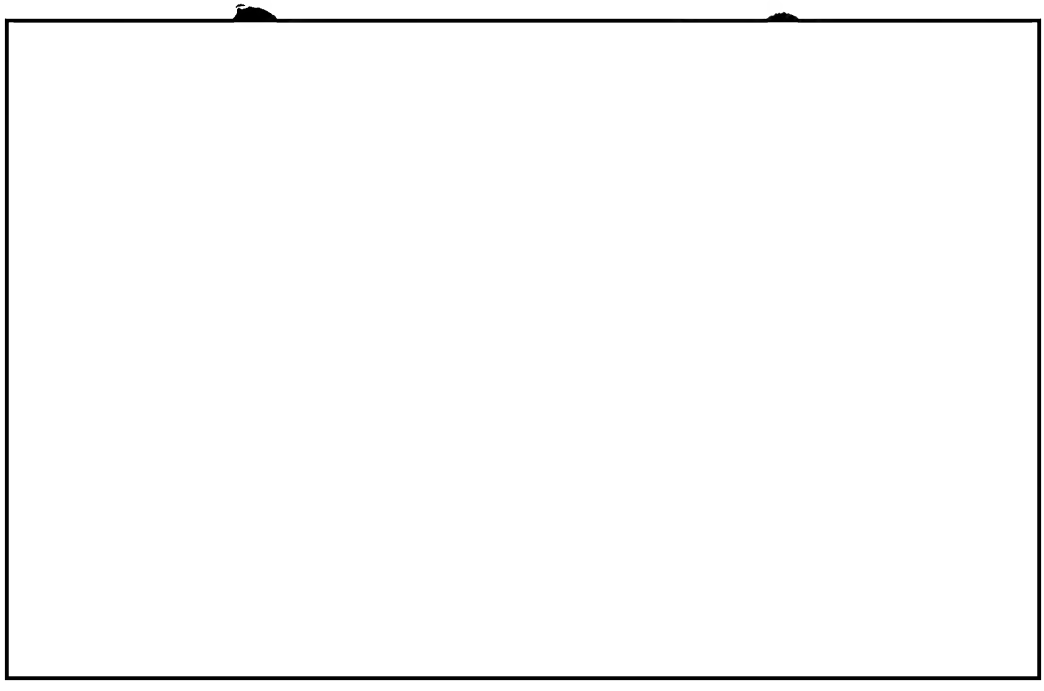
Date of Report: **11/24/2011**

Substantive Case File Number: 288A-AL-49289 ~~815I-AL-48391-Cyber~~

Source Reporting: On 11/24/2011, CHS emailed SA

b6
b7C
b7D

288A-AL-49289
- 8



b7D

Signed by:

Click here to sign this section

Signed by [redacted] View details
on Monday, November 28, 2011 2:05 PM (Eastern Daylight Time)

b6
b7C

Signed by [redacted] View details
on Tuesday, November 29, 2011 9:12 AM (Eastern Daylight Time)

FD-1023 (07/24/2010)	FEDERAL BUREAU OF INVESTIGATION

FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1324716-0

Total Deleted Page(s) = 50
Page 15 ~ b6; b7C;
Page 16 ~ b6; b7C;
Page 17 ~ b6; b7C;
Page 18 ~ b6; b7C;
Page 19 ~ b6; b7C;
Page 20 ~ b6; b7C;
Page 21 ~ b6; b7C;
Page 22 ~ b6; b7C;
Page 23 ~ b6; b7C;
Page 25 ~ b7E;
Page 26 ~ b7E;
Page 27 ~ b7E;
Page 28 ~ b7E;
Page 29 ~ b7E;
Page 30 ~ b7E;
Page 31 ~ b7E;
Page 32 ~ b7E;
Page 33 ~ b7E;
Page 34 ~ b7E;
Page 35 ~ b7E;
Page 36 ~ b7E;
Page 37 ~ b7E;
Page 38 ~ b7E;
Page 39 ~ b7E;
Page 40 ~ b7E;
Page 41 ~ b7E;
Page 42 ~ b7E;
Page 43 ~ b7E;
Page 44 ~ b7E;
Page 45 ~ b7E;
Page 46 ~ b7E;
Page 47 ~ b7E;
Page 48 ~ b7E;
Page 49 ~ b7E;
Page 50 ~ b7E;
Page 51 ~ b7E;
Page 54 ~ b7E;
Page 55 ~ b7E;
Page 56 ~ b7E;
Page 57 ~ b7E;
Page 58 ~ b7E;
Page 59 ~ b7E;
Page 60 ~ b7E;
Page 61 ~ b7E;
Page 62 ~ b7E;
Page 63 ~ b7E;
Page 64 ~ b7E;
Page 65 ~ b7E;

Page 66 ~ b7E;
Page 67 ~ b6; b7C;

XXXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXXXXX

108ebm01.ec

(Rev. 05-01-2008)

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 04/23/2012

To: Cyber **Attn:** SA [redacted] b6 b7C

Detroit **Attn:** SA [redacted]

From: Detroit
Grand Rapids RA/St. Joseph RA
Contact: SA [redacted]

Approved By: [redacted] b6 b7C

Drafted By: [redacted] (108ebm01.ec)

Case ID #: 288A-DE-106943 (Pending)

Title: UNSUB(S), AKA
Anonymous IRC,
Evil Security,
AntiSec Cutthroat Committee,
DeathToSnitches,
Anonymous,
Cutthroat,
LulzSec,
The LulzKnights;
BERRIEN COUNTY, MICHIGAN, GOVERNMNENT -
COMPUTER INTRUSION - CRIMINAL MATTER

Synopsis: EC to open [redacted] for captioned case. b7E

Enclosure(s): Copy of Berrien County Sheriff's Department report regarding incident number 2012-00004061 with several attachments.

Details: On 04/16/2012, SA [redacted] was contacted regarding captioned matter. Berrien County, Michigan, Sheriff's Department (BCSD) Detective [redacted] provided the details of the incident as well as the printed copy of the defacement of the Berrien County external website. Detective [redacted] explained that hackers had illegally entered the BCSD website and removed files without authorization while defacing the website. A copy of this defacement is attached to this EC. The defacement included the names Antisec Cutthroat Committee, #Antisec, #DeathToSnitches, #Anonymous, #Cutthroat, #LulzSec, The b6 b7C

O+A
FULL INVESTMENT
INITIATED 4-23-12
TO EXPIRE 10-22-12
TO: SA [redacted] b6 b7C
CAPTION:
4/26/12
288A-DE-106943 - 1

To: Cyber From: Detroit
Re: 288A-DE-106943, 04/23/2012

LulzKnights. The defacement also provided links to: https://twitter.com/AnonymousIRC and https://twitter.com/EvilSecurity. Additionally, a BCSD file listing usernames and passwords for users of the berriencounty.org website was compromised and taken. Numerous braggadocios statements were included with anti-government and anti-law enforcement comments.

Also on 04/16/2012, SA [redacted] and BCSD Detective [redacted] met with Berrien County [redacted] Michigan 49085, telephone number [redacted] advised that the BCSD external website was hosted by an outside internet contractor, E Internet Designs, in Kalamazoo, Michigan. Contact by [redacted] with this company determined that logs could possibly be obtained showing Internet Protocol (IP) addresses that accessed the victimized website around the time of the intrusion. Additionally, [redacted] advised that an unknown employee account had been set up in the name [redacted] around the time of the intrusion. [redacted] believed this to be a fictitious user account set up with administrative privileges so the hacker could re-enter the website. [redacted] provided a copy of the user accounts for the Berrien County website and put an asterisk next to the name of the fictitious account which was created on 04/15/2012, at 12:16 a.m. b6 b7C

Captioned FBI investigation should be opened to investigate this matter and determine the perpetrator(s) of this intrusion and defacement of the Berrien County internet website. The estimated economic loss will be calculated by [redacted] in relation to this incident. b6 b7C

To: Cyber From: Detroit
Re: 288A-DE-106943, 04/23/2012

LEAD(s):

Set Lead 1: (Action)

CYBER

AT WASHINGTON DC

For information and whatever action deemed appropriate.

♦♦

Berrien County Sheriff Case Report

Summary

Print Date/Time: 04/23/2012 12:25
Login ID: [redacted]
Case Number: 2012-00004061

BERRIEN COUNTY SHERIFF DEPARTMENT
ORI Number: MI1111100

Case

b6
b7C

Case Number: 2012-00004061
Location: 919 PORT
ST JOSEPH, MI 49085
Reporting Officer ID: 158 [redacted]

Incident Type: Damage to County Property
Occurred From: 04/14/2012 00:00
Occurred Thru: 04/15/2012 00:00
Disposition:
Disposition Date:
Reported Date: 04/17/2012 08:43 Tuesday

Offenses

No.	Group/ORI	Crime Code	Statute	Description	Counts
1	State	29000	2997	Computer Uses in Commission of	1
2	MI1111100	9939	9939	Computer Forensics Team	1

Subjects

Type	No.	Name	Address	Phone	Race	Sex	DOB/Age
Other	1	[redacted]	[redacted]		White	Female	
Other	2	E Internet Designs	UNKNOWN KALAMAZOO, MI				
Other	3	[redacted]	[redacted]		White	Male	
Victim	1	Berrien County Sheriff's Department	919 PORT ST JOSEPH, MI 49085	(269)983-7141			
Witness	1	[redacted]	[redacted]		White	Male	

b6
b7C

Arrests

Arrest No.	Name	Address	Date/Time	Type	Age

Property

Date	Code	Type	Make	Model	Description	Tag No.	Item No.
04/17/2012	Seized	07-Computer Hardware/Software			Lexar USB Drive, model N12610		

Vehicles

No.	Role	Vehicle Type	Year	Make	Model	Color	License Plate	State

ORIGINAL ASSIGNMENT:

On 04/15/12, R/O was contacted by [redacted] of the BCSD indicating that unknown individuals had entered onto the Berrien County Sheriff's Dept. website and removed all items that were placed onto the website and replaced those with their own items and also listing numerous e-mails and passwords for county employees.

b6
b7C

CONTACT WITH [redacted] OF THE BCSD:

Berrien County Sheriff Case Report

Summary

Print Date/Time: 04/23/2012 12:25 BERRIEN COUNTY SHERIFF DEPARTMENT b6
Login ID: [redacted] **ORI Number:** MI1111100 b7C
Case Number: 2012-00004061

On 04/15/12 at approximately 2100 hours, R/O contacted [redacted] via telephone, who indicated to R/O that on this date, he attempted to enter onto the BCSD website, which is identified as www.bcsheriff.org, at which time he observed that the website had been altered and none of the BCSD files could be accessed. It should be noted, [redacted] is an administrator for this website and assisted in building this website.

[redacted] at this time advised R/O that he began to view items that were listed on the website which neither he nor any employees had posted on there and observed there were several items referring to a group identified as Antisec, along with the group Anonymous.

Additionally, [redacted] advised he observed an e-mail list that had been posted on the site which had not been placed there by him or any other person legitimately accessing the site. In reviewing this e-mail list, he found that some of the e-mails contained names, passwords and e-mail addresses for numerous county employees, including judges and prosecutors. b6 b7C

[redacted] advised he did print out what he was able to from the site, which included approximately 40 pages of documents, along with the e-mail list. [redacted] indicated to R/O that he immediately contacted a supervisor to bring it to their attention that it appeared that the BCSD site had been accessed illegally and altered and that since that time he has attempted to re-access the site, however, it appears that it had been taken down by either the web page provider, which was identified as E Internet Designs or the Berrien County Computer Services.

[redacted] indicated he would forward a copy of the documents that he was able to print off prior to the site being taken off the internet.

REVIEW OF DOCUMENTS FROM [redacted] b6 b7C

On 04/16/12, R/O received a faxed copy of the items printed out by [redacted] In reviewing those items, the first couple items are texts that appear to be items placed onto the site from the individuals that illegally accessed the BCSD website.

At the top, it indicates Antisec Cutthroat Committees.
Below that it indicates Antisec Death to Snitches Anonymous Cutthroat and Lulz Sec

From there, R/O observes there are several sayings in reference to the Antisec fallen friends that possibly had been arrested in reference to what R/O believes is the same type of behavior. Further down on the second page it indicates Welcome to this new addition to the #SSS and (Shoot the Sheriff Sunday) signed by the Lulz Knights.

Below that it indicates bcsheriff.org mail in loot. After that it indicates several websites that individuals can follow the group responsible for this act on the internet. There are two Antisec crew Twitter sites which are identified as https://twitter.com/anonymousirc. The second is https://twitter.com/evilsecurity and a chat which is identified as irc.anonops.li#antisec.

On the next page, R/O observes that the individuals posted the user name for this site as Berrien C, with a password of [redacted] It should be noted, this is, in fact, believed to be the password for accessing the Sheriff's Dept. site, along with the password for E Internet Designs which is the designer of this webpage. b7E

The next group of files are numerous pages of e-mail user names/user ID's, passwords, and e-mail addresses. There are numerous pages of these which R/O has reviewed and observes that these are Sheriff's Dept./county employees, along with a lawyer group that conducts business through the Berrien County Courts.

On what R/O will refer to as page #16 (which is stamped at the top of the page via a fax machine), R/O observes that at the bottom of this page the last line indicates root+.pts/0 April 14th at 2333 hours 0048 32337 (Antisec). This is believed the approximate time where the illegal access to this site was taking place. The actual start date and time is not

Berrien County Sheriff Case Report

Summary

Print Date/Time: 04/23/2012 12:25 BERRIEN COUNTY SHERIFF DEPARTMENT
Login ID: [redacted] **ORI Number:** MI1111100
Case Number: 2012-00004061
known.

In further reviewing the items supplied to R/O by [redacted] R/O observed on page #25 and #26, several IP addresses that are shown and previous to these IP addresses, it indicates grant all privileges on root@65.183.182.120 along with IP address 99.155.145.32. R/O did check the IP addresses through the on-line search engine Geek Tools and found that the first IP address, being 65.183.182.120, is registered to the Internet service Raser-Tone out of Grand Rapids, MI. The second being 99.155.145.32, is registered to AT&T Internet Services. A copy of those look-ups will be attached to this report.

An additional IP address located by R/O is identified on page #37 of the information supplied by [redacted] That again is prefaced by grant all on to root@70.162.93.90 identified by E Internet Design, which appears to be the password for that company. It is spelled as follows: [redacted] R/O performed a "who is searched" on the on-line web service Geek Tools and found that the IP address 70.162.93.90 is registered to Cox Communications out of Atlanta, GA. A copy of that look-up will also be attached to this report.

A copy of the entire information that [redacted] supplied to R/O will be attached to this report.

TWITTER AND FACEBOOK SEARCHES:

R/O searched the Twitter account listed on the information that was placed onto the county website and in checking Antisec on Twitter, R/O found that Antisec appears to be associated with Anonymous, along with the Anonirc. R/O does observe some texts that appear to be similar from the Twitter account to the information that was uploaded to the Sheriff's Dept. website which is the saying "we are legion expect us". This is found on page #44 of the items supplied by [redacted] A copy of the Twitter page will be attached to this report also.

FACEBOOK INFORMATION:

R/O was supplied a copy of a Facebook posting under the URL https//www.facebook.com/antisecops. In reviewing the posting on that Facebook account, which appears to have the date of Monday at 4:26 a.m., Antisec shared a link Sunday and for other news for teh shit and giggles a handy defacement: http://www.bcsheriff.org/bahahahaantis3curityops. Below that it indicates Berrien County Sheriff's Department www.bcsheriff.org zip tips. There are several comments from people below, which the entire document will be attached to this report for review.

Again, at the back of the Facebook page under the mission statement of antis3curityops the text "we are legion expect us" is also seen on this site as in the information supplied to R/O by [redacted] For further details, see the attached Facebook document.

INTERVIEW WITH [redacted]

On 04/16/12 R/O, along with S/A [redacted] of the FBI, interviewed [redacted] in her office at the Berrien County Courthouse. [redacted] works in the Computer Services Dept. for the County of Berrien.

R/O supplied a copy of the information supplied to R/O by [redacted] to [redacted] and requested she review the e-mail addresses, along with the passwords that were posted on the Sheriff's Dept. website. [redacted] advised the R/O that this list appeared to be an older list of persons that had access to the Berrien County e-mail service, which several years ago used to be operated from the Sheriff's Dept. website. [redacted] advised R/O that this list is no longer valid and that the e-mail service does not operate out of the Sheriff's Dept. website any longer.

OFFICER NOTE:

R/O did check several of the e-mail and passwords with several employees to determine if these passwords were current and R/O was advised these were older passwords, approximately 4 to 5 years ago, and were no longer valid,

Berrien County Sheriff Case Report

Summary

Print Date/Time: 04/23/2012 12:25 BERRIEN COUNTY SHERIFF DEPARTMENT
Login ID: [redacted] **ORI Number:** MI1111100
Case Number: 2012-00004061

which is consistent with what [redacted] observed from the information supplied to her by R/O. b6 b7C

[redacted] indicated to R/O that the webpage for the Berrien County Sheriff's Office, along with the County of Berrien, are sister pages that are maintained by the web service E Internet Designs and are maintained by that company. At this time R/O was supplied two contact names and numbers being [redacted] of E Internet Designs at [redacted] and [redacted]

[redacted] advised R/O that once it was discovered that the Sheriff's Dept. webpage had been accessed and changed illegally, she contacted the internet and the webpage was taken out of service. [redacted] advised R/O's that she then searched who had accessed the Berrien County site recently and observed a name and date that was somewhat suspicious to her. This was identified as a [redacted] who last accessed the website on 04/15/12 at 0016 hours. [redacted] advised R/O that she has checked with E Internet Designs and has determined that [redacted] if not an employee of E Internet Designs and is not an employee or valid user from the County of Berrien. [redacted] advised she has not deleted this account, however, has changed the password for that user so that he is unable to access that account.

It should be noted, that 04/15/12 at 0016 hours is on or about the time that it appears the illegal access to the website took place.

CONTACT WITH [redacted]

While in [redacted] office, she made contact with [redacted] via telephone and a conference call took place via speaker phone with him. b6 b7C

[redacted] indicated that his company, E Internet Designs was able to capture the log files for the date and time in question and indicated he would supply a copy of all those log files to this department for follow-up investigation. It should be noted, during the conversation with [redacted] the actual County of Berrien had also been accessed by the suspects, however, the only defacement that took place on the County of Berrien site was several links were placed onto the webpage which have been since removed by [redacted] These web links were similar to those posted on the Sheriff's Dept. site by the suspects.

FILES RECEIVED FROM E INTERNET DESIGNS:

On 04/19/12, R/O received a USB flash drive from E Internet Designs and downloaded that file to R/O's computer. In reviewing those files, R/O reviewed the accessed log file for the approximate date and time that this incident took place, however, was not able to locate any visible suspects from the access log file.

R/O has re-contacted [redacted] at E Internet Designs for assistance in going through the remainder of the files which are approximately 10GB in size with one of the E Internet Designs techs to see if any useful information can be obtained from the additional files. b6 b7C

INFORMATION FROM S/A [redacted] OF THE FBI: b6 b7C

R/O has been in contact with S/A [redacted] who took part in the interview with [redacted] S/A [redacted] indicated that his agency has an open case on the groups Anonymous and Antisec and that his agency would be willing to assist in the investigation of this complaint.

OFFICER'S REMARKS:

During the initial assessment of what the suspects had done on the Berrien County Sheriff's website, it was believed that all files had been removed by the suspects, along with all backup files. However, upon further examination, backup files were located by E Internet Designs and the Berrien County Sheriff's website has been reinstated in full and it does not appear that any of the original files are missing.

Berrien County Sheriff Case Report

Summary

Print Date/Time: 04/23/2012 12:25
Login ID: [redacted]
Case Number: 2012-00004061

BERRIEN COUNTY SHERIFF DEPARTMENT
ORI Number: MI1111100

b6
b7C

STATUS:

This complaint remains open and under investigation.

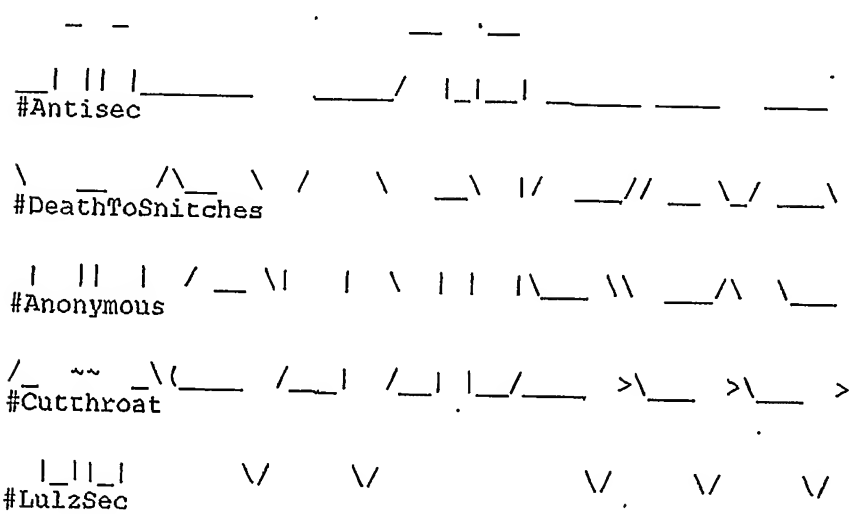
Reviewed By **Date**

Dispo Code **Date**

Assigned To **Date**

Routing:

AntiSec Cutthroat Cummittee



#ANTISEC SlAPPING YOUR SECURITY WITH OUR COCKS**

LOVE TO LULZSEC / ANTISEC FALLEN FRIENDS

THOSE WHO TRULY BELIEVED WE COULD MAKE A DIFFERENCE

LOVE TO THOSE BUSTED ANONS, FRIENDS WHO ARE FIGHTING FOR THEIR OWN FREEDOM NOW

LOVE TO THOSE WHO FIGHTED FOR THEIR FREEDOM IN TUNISIA, EGYPT, LIBYA

SYRIA, BAHRAIN, YEMEN, IRAN, ETC AND ETC AND ETC

LOVE TO THOSE WHO FOUGHT FOR FREEDOM OF SPEECH, FOR A REAL DEMOCRACY,

FOR A GOVT FREE OF CORRUPTION,

FOR A FREE WORLD WHERE WE ARE ABLE TO SHARE OUR KNOWLEDGE FREELY

LOVE TO THOSE WHO FIGHT FOR SOMETHING THEY BELIEVE IN

WE ARE ANTISEC

WE LL FIGHT TILL THE END

WE ARE THE KNIGHTS OF THE LULZ,

WE INHABIT YOUR DREAMS AND SHADOWS.

hello dear friends!

Welcome to this new edition of #SSS (Shoot the Sheriff Sunday)

- The LulzKnights.

ALL YOUR BASE ARE BELONG TO

[redacted]

/* And so I am become a knight of the Kingdom of Dreams and Shadows (- Mark Twain)

/* bcsheriff.org Mail and Loot

Follow the Antisec Crew: https://twitter.com/AnonymousIRC

Follow the Antisec Crew: https://twitter.com/EvilSecurity

Chat: irc.anonops.li #antisec

[redacted]

The Unknown

As we know,

There are known knowns.

There are things we know we know.

We also know

There are known unknowns.

That is to say

We know there are some things

We do not know,

But there are also unknown unknowns,

The ones we don't know

We don't know.

D.R.Rumsfeld

(American poet and drag queen)

[redacted]

Plain Text? and they call what we do a crime.. nomnomnonmonm

```
$hostname_systemDB = "localhost";

$database_systemDB = "berriencounty_test_org";

$username_systemDB = "berrienc";

$password_systemDB = "b3rr13nc";


$hostname_rsSupport = "localhost";

$database_rsSupport = "einternetdesign_com";

$username_rsSupport = "eid_domain_user";
```

b7E

$password_rsSupport = [redacted]

```
+------------------+--------------+-------------------------------+-------
--+
| username         | password     | email_address                 |
user_id |
+------------------+--------------+-------------------------------+-------
--+
```

[redacted]

1 |

[redacted] | NULL |

b6
b7C

[redacted]

b6
b7C

[redacted] | NULL

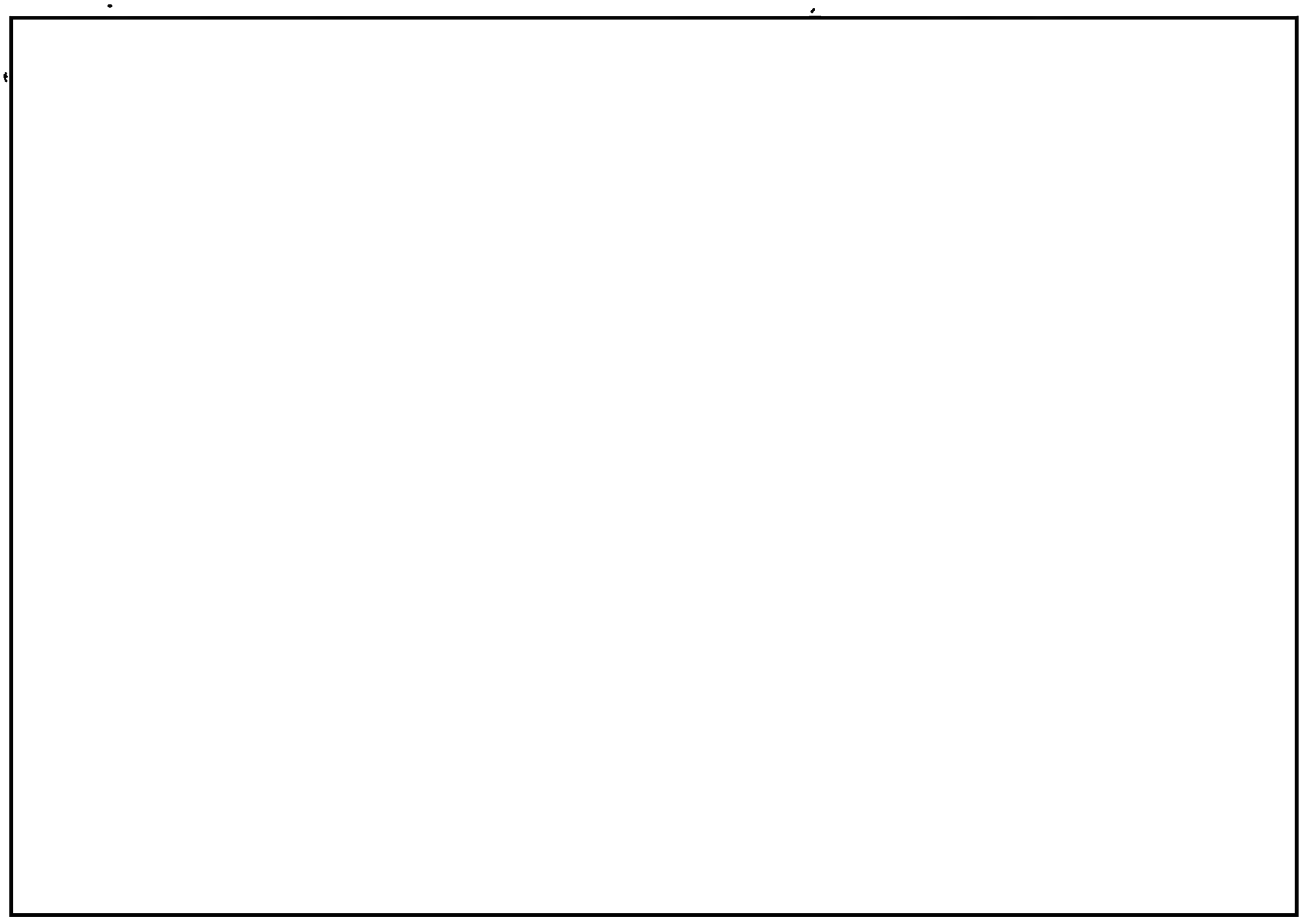
[redacted]

can i haz candiez?

:3

[redacted]

b7E



b7E

pwn'd thankyou

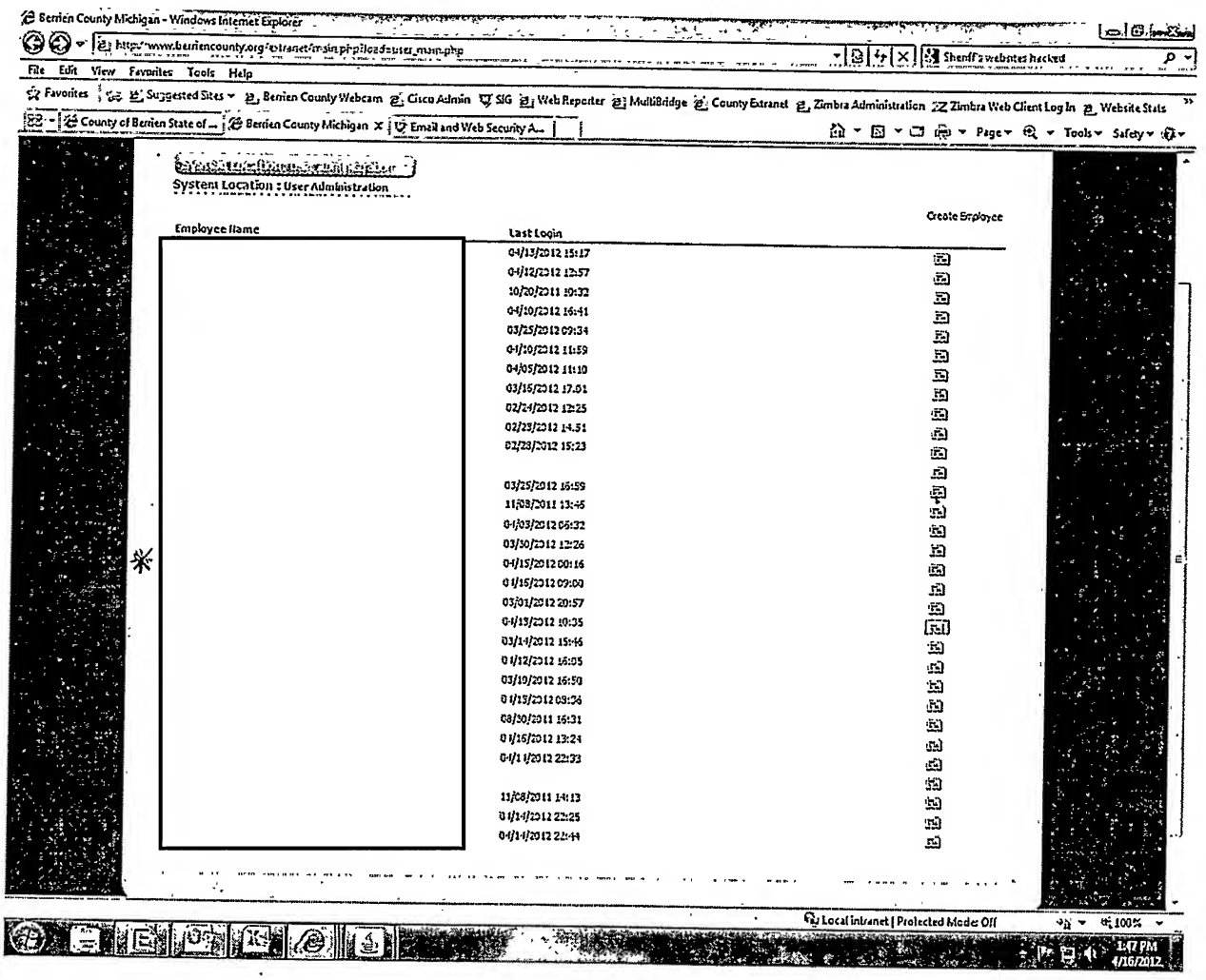
EAT COCK

We are Legion

We do not forgive

We do not forget

Expect Us


Berrien County Michigan - Windows Internet Explorer
http://www.berriencounty.org/intranet/main.php?load=user_main.php
Sheriff's websites hacked
File Edit View Favorites Tools Help
Favorites
Suggested Sites
Berrien County Webcam
Cisco Admin
SIG
Web Reporter
MultiBridge
County Extranet
Zimbra Administration
Zimbra Web Client Log In
Website Stats
County of Berrien State of ...
Berrien County Michigan
Email and Web Security A...
Page
Tools
Safety
System Location : User Administration
Employee Name
Last Login
Create Employee
04/13/2012 15:17
04/12/2012 12:57
10/20/2011 10:32
04/10/2012 16:41
03/25/2012 09:34
04/10/2012 11:59
04/05/2012 11:10
03/16/2012 17:01
02/24/2012 12:25
02/23/2012 14:51
02/23/2012 15:23
03/25/2012 16:59
11/08/2011 13:46
04/03/2012 05:32
03/30/2012 12:26
04/15/2012 00:16
04/15/2012 09:00
03/01/2012 20:57
04/13/2012 10:35
03/14/2012 15:46
04/12/2012 16:05
03/19/2012 16:50
04/15/2012 09:36
08/30/2011 16:31
04/16/2012 13:24
04/11/2012 22:33
11/08/2011 14:13
04/14/2012 22:25
04/14/2012 22:44
Local intranet | Protected Mode: Off
100%
1:47 PM
4/16/2012

b6
b7C

CLOSE Fw: Anonymous "Anthony V. + Add to Adk

Sent By: "[redacted]@ic.fbi.gov> On:Apr 04/24/12 10:26 AM
To: "[redacted]@comcast.net>

b6
b7C

Possible hacker lead.

----- Original Message -----
From: [redacted]
To: [redacted]
Cc:
Sent: Thu Apr 19 21:50:42 2012
Subject: Re: Anonymous

b6
b7C

SA [redacted] here is what I have from a sub-source:

One of our analysts observed what looks like a dump of data from the Berrien, MI Sherriff's office on Pastebin.

http://pastebin.com/raw.php?i=bydTpuQ9

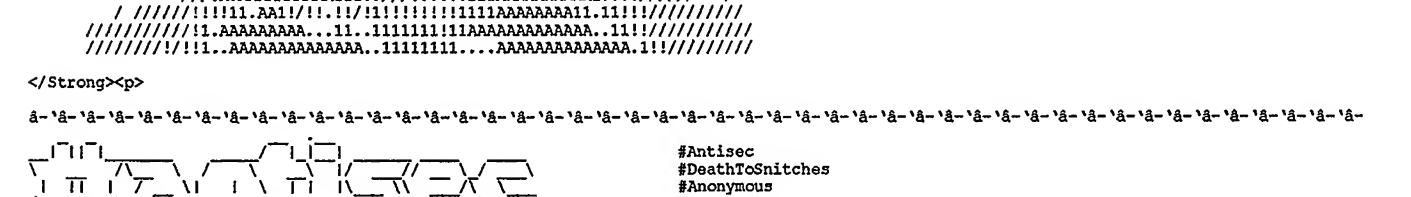
The dump itself hosted at depositfiles.com (http://depositfiles.com/files/1s2zz3uvs) and consists of a ~44m tarball. Purportedly contains public records as well LE-sensitive info.

----- Original Message -----
From: [redacted]
To: [redacted]
Cc:
Sent: Thu Apr 19 21:47:48 2012
Subject: Re: Anonymous

b6
b7C

b7E

```
</Strong><p>
```



#ANTISEC SlAPPING YOUR SECURITY WITH OUR COCKS++

LOVE TO LULZSEC / ANTISEC FALLEN FRIENDS
THOSE WHO TRULY BELIEVED WE COULD MAKE A DIFFERENCE
LOVE TO THOSE BUSTED ANONS, FRIENDS WHO ARE FIGHTING FOR THEIR OWN FREEDOM NOW
LOVE TO THOSE WHO FIGHTED FOR THEIR FREEDOM IN TUNISIA, EGYPT, LIBYA
SYRIA, BAHRAIN, YEMEN, IRAN, ETC AND ETC AND ETC
LOVE TO THOSE WHO FOUGHT FOR FREEDOM OF SPEECH, FOR A REAL DEMOCRACY,
FOR A GOVT FREE OF CORRUPTION,
FOR A FREE WORLD WHERE WE ARE ABLE TO SHARE OUR KNOWLEDGE FREELY
LOVE TO THOSE WHO FIGHT FOR SOMETHING THEY BELIEVE IN
WE ARE ANTISEC
WE LL FIGHT TILL THE END
WE ARE THE KNIGHTS OF THE LULZ,
WE INHABIT YOUR DREAMS AND SHADOWS.

~
hello dear friends!

Welcome to this new edition of #SSS (Shoot the Sheriff Sunday)

- The LulzKnights.

ALL YOUR BASE ARE BELONG TO

â-'â-'â-'

(Rev. 05-01-2008)

~~CONFIDENTIAL//FGI ROU/REL~~ TO USA, ROU

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/10/2012

To: Cyber **Attn:** [redacted]

Jacksonville **Attn:** SSA [redacted]
SA
SA

International Operations **Attn:** Eurasia Unit, SSA [redacted]

b6
b7C

From: Bucharest
Contact: ALAT [redacted]

Approved By: [redacted]

Drafted By: [redacted] :ap

Case ID #: [redacted] (Pending)
(Pending)

b7A

(C) **Title:** [redacted]

(C) [redacted]

~~**Derived From :** Multiple Sources~~
~~**Declassify On:** 20370510~~

(C) [redacted]

b1
b3

(C) [redacted]

~~CONFIDENTIAL//FGI ROU/REL~~ TO USA, ROU

288A-DE-106943 - 3

To: Cyber From: Bucharest
Re: [redacted] 05/10/2012

b7A

(C)

b1
b3

To: Cyber From: Bucharest
Re: [redacted] 05/10/2012

b7A

(C)

[redacted]

b1
b3

To: Cyber From: Bucharest
Re: [redacted] 05/10/2012

b7A

LEAD(s):

Set Lead 1: (Info)

CYBER

AT CCU-1, DC

Read and clear.

Set Lead 2: (Info)

JACKSONVILLE

AT JACKSONVILLE, FL

Read and clear.

Set Lead 3: (Info)

INTERNATIONAL OPERATIONS

AT EURASIA UNIT, DC

Read and clear.

♦♦

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

DATE: 03-07-2013
CLASSIFIED BY NSICG/J9674T52
REASON: 1.4 (c, d)
DECLASSIFY ON: 03-07-2038

From: [redacted](BO)(FBI)
Sent: Thursday, May 10, 2012 3:35 AM
To: [redacted]

(C) **Subject:** More Anonymous inf[redacted]

Classification: CONFIDENTIAL//FGI ROU//REL TO USA, ROU

Classified By: F77M68K14
Declassify On: 20370510
Derived From: FBI NSISC-20090615

All,

(C) Here's the latest from [redacted] they've been pretty busy. Please note the classification.

There are a number of new US victims, including .mil, and plans for future targeting, like centcom.mil. (I'm sure you know people over there[redacted]:-)

(C) [redacted]

[redacted]
Assistant Legal Attaché
Legat Bucharest (Romania, Moldova)

Office: [redacted]
Mobile: [redacted]bic.fbi.gov

Classification: CONFIDENTIAL//FGI ROU//REL TO USA, ROU

Classification: CONFIDENTIAL//FGI ROU//REL TO USA, ROU

Classification: CONFIDENTIAL//FGI ROU//REL TO USA, ROU

Classification: CONFIDENTIAL//FGI ROU//REL TO USA, ROU

288A-DE-106943-4

From: [redacted] (BO)(FBI)
Sent: Friday, May 11, 2012 9:53 AM
To: [redacted]
Cc: [redacted]
Subject: RE: More Anonymous info [redacted]

b6
b7C
b1
b3

(C)

Classification: CONFIDENTIAL//FGI ROU//REL TO USA, ROU

Classified By: F77M68K14
Declassify On: 20370511
Derived From: FBI NSISC-20090615
==========

Thanks for the introduction [redacted]

[redacted]

b6
b7C
b7E

Classification: CONFIDENTIAL//FGI ROU//REL TO USA, ROU

==========
Classification: CONFIDENTIAL//FGI ROU//REL TO USA, ROU

==========
Classification: CONFIDENTIAL//FGI ROU//REL TO USA, ROU

288A-OE-106943-5

From: [redacted] (BO)(FBI)
Sent: Friday, May 11, 2012 9:53 AM
To: [redacted] b6 b7C
Cc: [redacted]
(C) **Subject:** RE: More Anonymous in [redacted] b1 b3

Classification: CONFIDENTIAL//FGI ROU//REL TO USA, ROU

From: [redacted]
Sent: Friday, May 11, 2012 4:10 PM
To: [redacted] b6 b7C
Cc: [redacted]
(C) **Subject:** FW: More Anonymous inf [redacted] b1 b3

Classification: CONFIDENTIAL//FGI ROU//REL TO USA, ROU

Classified By: F43M81K92
Declassify On: 20370511
Derived From: FBI NSISC-20090615
==========

(C) Thanks very much [redacted]

[redacted] b1 b3 b6 b7C

Thanks guys,

[redacted]

==========
Classification: CONFIDENTIAL//FGI ROU//REL TO USA, ROU

==========
Classification: CONFIDENTIAL//FGI ROU//REL TO USA, ROU

288A-DE-106943 - 6

FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1324716-0

Total Deleted Page(s) = 2
Page 16 ~ b7E;
Page 17 ~ b7E;

XXXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXXXXX

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 08/22/2011

On 08/17/2011, investigating agent electronically emailed [redacted] an electronic copy of a Federal Grand Jury Subpoena for [redacted] b3 b6 b7C

Later the same day, [redacted] electronically replied that [redacted] had received the aforementioned subpoena. b6 b7C

Investigation on 08/17/2011 at Santa Ana, California

File # 288A-LA-258335-1 Date dictated

by SA [redacted] b6 b7C

234jhF01.wpd

b6
b7C

FD-340 (Rev. 4-11-03)

File Number 288A-LA-258335-1A1

Field Office Acquiring Evidence Los Angeles

Serial # of Originating Document 3

Date Received 07/26/2011

From [redacted]
(Name of Contributor/Interviewee)

(Address)

(City and State)

By SA [redacted]

To Be Returned ☐ Yes ☒ No

Receipt Given ☐ Yes ☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e) Federal Rules of Criminal Procedure

☐ Yes ☒ No

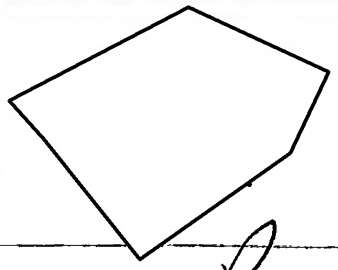
Federal Taxpayer Information (FTI)

☐ Yes ☒ No

Title:

Reference:
(Communication Enclosing Material)

Description: ☒ Original notes re interview of [redacted] on 07/26/2011



7/26/2011

1 week @ one-West Bank

b6
b7C

Received email

- Lulz Sec

- I am the DDOS

8/1/2011

for 1 month

to put One-West Bank out of business

2nd - two (2) Internet Point of Access - own [redacted] - [redacted]

1st - Sequel injection Attacks to get confidential information

Robo - Signing Scandal - may be reason

bacteria or virus Yahoo acct: arcanobacter7@yahoo.com

[redacted] @ owb.com

b6
b7C

Will redirect DDOS thru Qwest

(Rev. 05-01-2008)

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 07/26/2011

To: Los Angeles

From: Los Angeles
Squad [redacted]
Contact: SA [redacted]

b6
b7C

Approved By: [redacted]

Drafted By: [redacted]:jhf

Case ID #: 288A-LA-258335 (Pending) - 2

NTP014
CRI-CRINT-F

Title: LULZSEC - SUBJECT(S);
ONEWEST BANK - VICTIM
COMPUTER INTRUSION
OO:LA

Synopsis: Request that the captioned matter be opened and assigned to the investigating agent.

Details: On 07/26/2011, writer received information indicating that OneWest Bank was being targeted by LulzSec for a DDoS attack. Additional information indicated that the computer security contact at OneWest Bank was [redacted] at [redacted]

b6
b7C

On 07/26/2011, writer telephonically contacted [redacted] confirmed that OneWest had received an email, signed by LulzSec. In the email, LulzSec indicated that they intended to launch a month-long DDoS attack against OneWest. Additional information regarding [redacted] interview can be found in an associated FD-302.

b6
b7C

Based on the aforementioned information, writer requests that the captioned matter be opened and assigned to the writer.

♦♦

UNCLASSIFIED

O & A
SA [redacted]
8/25/11

b6
b7C

207jhf02.wpd

288A-LA-258335-2

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 07/27/2011

On 07/26/2011, [redacted] for OneWest Bank, email address of [redacted]owb.com, business telephone number of [redacted] and cellular telephone number of [redacted] was telephonically contacted at his business telephone number. After being advised of the identity of the investigating agent and the nature of the interview, the following information was provided: b6 b7C

[redacted] has been working for OneWest for about seven (7) weeks.

[redacted] stated that OneWest had received an email from a group identified as LulzSec. In the email, LulzSec indicated that they were going to launch a month-long DDoS attack against OneWest Bank and try to put OneWest Bank out of business. The email also indicated that the DDoS attack would be launched on 08/01/2011.

b6 b7C

The LulzSec email appears to have originated from a Yahoo account of arcanobacter7@yahoo.com. [redacted] or someone at OneWest had done some research and determined that the word arcanobacter originated from a word describing some type of bacteria or virus.

[redacted] had information indicating that LulzSec would first utilize a sequel injection attack to obtain confidential information from the OneWest Bank computer systems. Next, LulzSec was likely to launch a DDoS attack against OneWest Bank's computer systems.

[redacted] stated that OneWest Bank has computer servers at two (2) primary facilities. One (1) computer facility is located in [redacted] and the second facility is located in [redacted] suspected that the DDoS attack would be launched at one or both of these facilities.

b6 b7C

[redacted] and the OneWest Bank organization have contracted with an Internet security company called Qwest to have Qwest re-direct the large majority of DDoS traffic that LulzSec might direct at OneWest Bank servers.

[redacted] suggested that LulzSec might be targeting OneWest Bank because of OneWest Bank's involvement with the Robo-Signing

Investigation on 07/26/2011 at Santa Ana, California (telephonically)

File # 288A-LA-258335-3 Date dictated

by SA [redacted]

b6 b7C

b6
b7C

Loan Scandal. OneWest Bank and several other banks had been implicated in the Robo-Signing Loan Scandal. LulzSec might see themselves as a defender of public interest. Hence, LulzSec might see a DDoS attack against OneWest Bank as a means to vindicate those people affected by the Robo-Signing Loan Scandal. [redacted] was not aware of any other reasons why LulzSec would single out OneWest Bank for a DDoS attack.

b6
b7C

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 08/22/2011

On 08/22/2011, investigating agent received information confirming that a copy of a Federal Grand Jury Subpoena for [redacted] at 12:57:52 PDT had been faxed to [redacted]

b3
b6
b7C

Investigation on 08/22/2011 at Santa Ana, California

File # 288A-LA-258335-4 Date dictated

by SA [redacted]

b6
b7C

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 07/27/2011

On 07/26/2011, [redacted] for OneWest Bank, business address of 888 East Walnut Street, Pasadena, California, 91101, email address of [redacted]@owb.com, business telephone number of [redacted] and cellular telephone number of [redacted] emailed the investigating agent the following information: b6 b7C

[redacted] forwarded a copy of the email received from LULZSEC. The subject of the email referred to "payback for your banking practices". The body of the email referred to LulzSec launching a month long DDoS against OneWest Bank to put OneWest out of business. The email was dated July 19, 2011.

A printout of the email is attached to this document.

(X)

D.H.T.

Investigation on 07/27/2011 at Santa Ana, California

File # 288A-LA-258335-5 Date dictated

by SA [redacted] b6 b7C

208jhfo1.wpd

288A-LA-258335-5

payback for your banking practices

Arcanobacter Hemolyticum [arcanobacter7@yahoo.com]

Sent: Tuesday, July 19, 2011 12:57 PM

To: OWB-CREG-Service [OWB-CREG-Service@owb.com]

come Aug 1, we plan to launch a month long DDOS and put you slimeballs out of business.

HACKERS UNITE !!

LULZSEC

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 08/05/2011

On 08/01/2011, [redacted] for OneWest Bank, business address of 888 East Walnut Street, Pasadena, California, 91101, email address of [redacted]owb.com, business telephone number of [redacted] and cellular telephone number of [redacted] emailed the investigating agent the following information: b6 b7C

OneWest Bank employees [redacted] were also recipients of the email.

In the body of the email, [redacted] noted that there has been an increase in reconnaissance activities directed at the OneWest Bank computers. In particular, there have been about 1000 plus reconnaissance probes from Chinese Internet Protocol (IP) addresses. [redacted] noted that actual DDoS attacks are preceded by reconnaissance attacks. [redacted] further describes steps that OneWest Bank is taking to address issues related to a suspected DDoS attack. Details of these steps are provided in the body of [redacted] email. b6 b7C

A printout of the email is attached to this document.

Investigation on 08/05/2011 at Santa Ana, California

File # 288A-LA-258335-6 Date dictated

by SA [redacted] b6 b7C

217 information

LulzSec Update

[@owb.com]

Sent: Monday, August 01, 2011 1:34 PM

To:

Cc:

b6
b7C

Hell

Just a quick update on where we currently stand:

b6
b7C

1) We have not seen an increase in unusual activity other than the penetration testing that are doing. They started this work last Saturday.

b7E

2) We have seen an increase in reconnaissance activities, specifically about a 1000 plus probes coming from a Chinese IP address which we are watching, but as yet nothing has materialized. We will have the It should be noted that all actual attacks are preceded by reconnaissance attacks

3) Our target completion date for these remediation activities is COB on Wednesday August 3, 2011

b7E

4) We are in the process of removing all systems from the that do not need to be there

5) They should have these vulnerabilities remediated by COB on Wednesday August 3, 2011

b6
b7C
b7E

6) We are waiting for a confirmation on the pricing and hope to have this information by COB tomorrow, Tuesday. We will then need approval to purchase

7) The network Risk Assessment has been completed and we are focusing on the critical and high risk items first

8) The database scanning has been completed and the vulnerabilities have been turned over to the database teams to fix. We have asked the databases team to get back to us with a remediation plan by COB today.

b7E

I will be sending out updates to everyone on a daily basis.

Please let me know if you have any questions
Best regards

One West Bank
888 East Walnut Street
Pasadena, CA 91101
Work.....
Cell.....
e-mail:.....

b6
b7C

FD-919 (Rev. 06-05-2003)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 12/21/2011

To: Los Angeles

From: Los Angeles [redacted] b6 b7C
Contact: SA [redacted]

Approved By: [redacted] 12/21/11

Drafted By: [redacted] b6 b7C

Case ID #: [redacted] (Pending) -7
[redacted] (Pending) -20441 b7A

Title: VICTIM NOTIFICATION FORM

Synopsis: Victim contact information

Reference: 288A-LA-258335 Serial 1

Details:

VnsCase#: 288A-LA-258335
CAgtName: [redacted] b6 b7C
PContact: Business
BusName : Onewest Bank
BusEIN :
BusAcct :
VicFirN : Security
VicMidN :
VicLastN: Chief
SSAN :
VicDate : 20110726
VicDOD :
VicMinor:
DOB :
Race :
Sex :
Addr :
Addr2 :
City :
State : CA
Country : US
Zip :
Email :
HPhone :
Fax :

355 tm03.11

288A-LA-258335-7

VWrkAddr: 888 East Walnut St
VWrkadd2:
VWrkCity: Pasadena
VWrkSt : CA
VWrkCtry: US
VWrkZip : 91101
WEmail :
WPhone : 6265354451
WFax :
VicPager:
NOKFirN :
NOKMidN :
NOKLastN:
NOKRel :
NOKAddr :
NOKAddr2:
NOKCity :
NOKState:
NOKCtry :
NOKZip :
NOKHEmal:
NOKWEmal:
NOKHPho :
NOKWPho :
NOKHFax :
NOKWFax :
NOKPager:
GrdFirN :
GrdMidN :
GrdLastN:
GrdRel :
GrdAddr :
GrdAddr2:
GrdCity :
GrdState:
GrdCtry :
GrdZip :
GrdHEmal:
GrdWEmal:
GrdHPho :
GrdWPho :
GrdHFax :
GrdWFax :
GrdPager:
PropRet : N
TotLoss : 000000000
Lang. :
Disable :

♦♦

(Rev. 05-01-2008)

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 01/18/2012

To: Los Angeles

From: Los Angeles
[redacted]
Contact: SA [redacted]

b6
b7C

Approved By: [redacted] 2/8/12

Drafted By: [redacted] :jhf

Case ID #: 288A-LA-258335-8 (Pending)

Title: LULZSEC - SUBJECT(S);
ONEWEST BANK - VICTIM
COMPUTER INTRUSION
OO:LA

Synopsis: Request that captioned investigation be closed administratively.

Details: Writer requests that captioned investigation be closed administratively. Subject(s) threatened to launch a Denial-Of-Service (DDoS) attack against OneWest Bank computers. A DDoS attack was never launched against OneWest Bank's computers and consequently OneWest did not sustain a significant financial loss. Therefore, this investigation does not meet the minimal loss amount guidelines for a Federal violation

Writer has verified that there are no 1B, 1C or 1D items assigned to the captioned investigation. Therefore, there is no need for a disposition of evidence.

Consequently, writer requests that the captioned investigation be closed administratively.

♦♦

UNCLASSIFIED

2/9/12

288A-LA-258335-8

FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1324716-0

Total Deleted Page(s) = 23
Page 5 ~ b7D; b7E;
Page 7 ~ b6; b7C; b7D;
Page 8 ~ b6; b7C; b7D;
Page 12 ~ b6; b7C; b7D; b7E;
Page 13 ~ b7D; b7E;
Page 14 ~ b7E;
Page 15 ~ b7E;
Page 16 ~ b7E;
Page 17 ~ b6; b7C; b7D; b7E;
Page 18 ~ b7E;
Page 20 ~ b6; b7A; b7C; b7D; b7E;
Page 21 ~ b7A; b7D; b7E;
Page 22 ~ b7E;
Page 23 ~ b7E;
Page 24 ~ b7E;
Page 25 ~ b7E;
Page 26 ~ b7E;
Page 27 ~ b7E;
Page 28 ~ b7E;
Page 29 ~ b7E;
Page 30 ~ b7E;
Page 31 ~ b7E;
Page 33 ~ b6; b7C; b7D;

XXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXXXX

(Rev. 05-01-2008)

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 06/06/2011

To: Tampa

From: Tampa
[redacted]
Contact: SA [redacted] b6 b7C

Approved By: [redacted]

Drafted By: [redacted] arm

Case ID #: 288A-TP-NEW (Pending)
73999 -1

Title: LULZSEC - SUBJECT
COMPUTER INTRUSION - CRIMINAL

INDEX
INITIALS

Synopsis: Open and assign case.

Details: Writer has developed CHS [redacted] b7D
[redacted] internet hacker group LULZSEC. LULZSEC is believed to be a splinter group of Anonymous. Anonymous is a global hacking group which has committed computer intrusions into many U.S. businesses and government groups.

[redacted] b7D is providing significant information on the identity of the members of LULZSEC.

Writer requests to open and assign case.

♦♦

UNCLASSIFIED

Q+A to ✓
SA [redacted] b6 b7C

0606 ARM01.ec

(Rev. 05-01-2008)

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 06/06/2011

To: Cyber **Attn:** CCU
ASC
SSA

b6
b7C

From: Tampa
Squad 8/Cyber
Contact: SA

Approved By:

Drafted By: arm

Case ID #: 288A-TP-73999 (Pending) -2

Title: LULZSEC - SUBJECT
COMPUTER INTRUSION - CRIMINAL

Synopsis: Request case funds.

Details: Writer requests funds for the support of captioned investigation.

FBI Tampa has developed a CHS who is currently reporting on LULZSEC splinter group of Anonymous.

b7D

b7D

In order to successfully operate CHS and

b7D
b7E

UNCLASSIFIED

0606ARM02.ec

To: Cyber From: Tampa
Re: 288A-TP-73999, 06/06/2011

LEAD(s):

Set Lead 1: (Action)

CYBER

AT CCU-1

Transfer requested funds to [redacted] b7E

♦♦

Precedence: ROUTINE Date: 06/16/2011

To: Cyber Attn: CCS/CCU
SSA
SSA
SSA

Charlotte Attn: ASAC
ASAC
SSA

New York Attn: SA
SA

Tampa Attn: SA

b6
b7C

From: Charlotte
Squad 7/Cyber
Contact: SA
SA

Approved By:

Drafted By:

b6
b7C

Case ID #: (Pending)
288A-TP-73999 (Pending)

Title:

b7A

LULZSEC - SUBJECT;
COMPUTER INTRUSION - CRIMINAL
(288A-TP-73999)

Synopsis: This Electronic Communication (EC) will document a joint Charlotte, Tampa and New York Division Operation to utilize

b7D
b7E

Details: have been extensively engaged in

b7D

b7A

(Rev. 05-01-2008)

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 06/30/2011

To: Cyber **Attn:** CCS/CCU
SSA
SSA
SSA

Charlotte **Attn:** ASAC
ASAC
SSA

New York **Attn:** SA
SA

Tampa **Attn:** SA

b6
b7C

From: Charlotte
CY-1/Cyber
Contact: SA
SA

Approved By:

Drafted By: :pja PSA

Case ID #: (Pending)
288A-TP-73999 (Pending) -10

b7A

Title:

LULZSEC - SUBJECT;
COMPUTER INTRUSION - CRIMINAL
(288A-TP-73999)

Synopsis: To document the approval of Charlotte and Tampa CHSs for

b7D
b7E

Reference:
288A-TP-73999 Serial 4

b7A

UNCLASSIFIED

File Copy

UNCLASSIFIED

FD-1023 (07/24/2010)	FEDERAL BUREAU OF INVESTIGATION CHS REPORTING DOCUMENT

HEADER

Source ID: [redacted]

Date: **06/16/2011**

Case Agent Name: [redacted]

Field Office/Division: **Tampa**

Squad: **SQUAD EIGHT**

b6
b7C
b7D

Date of Contact: **06/16/2011**

List all present including yourself. (Do not include the CHS.): Writer

Type of Contact: **e-Mail**

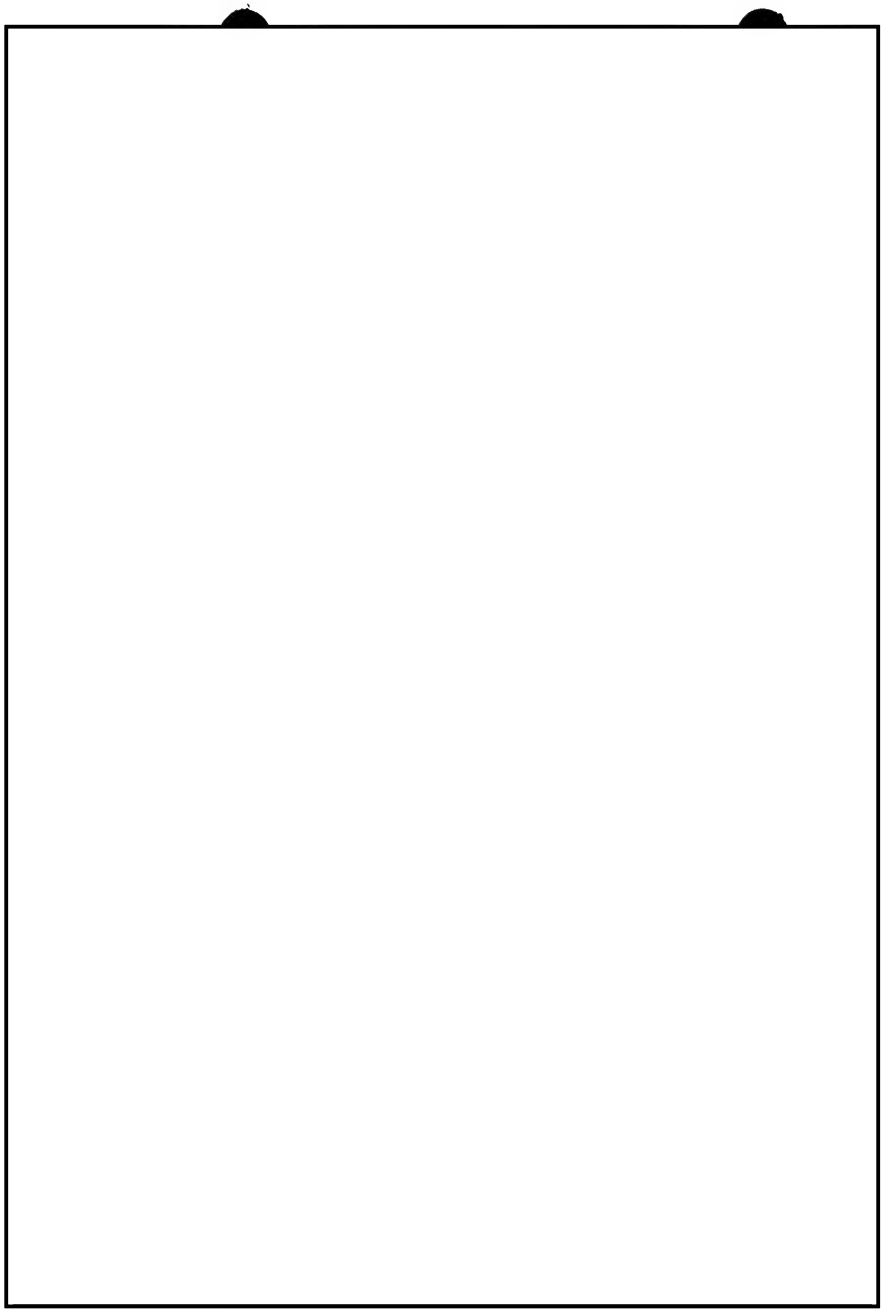
Date of Report: **06/16/2011**

Substantive Case File Number: **288A-TP-73999** ~21

Source Reporting: CHS provided writer with [redacted]

b6
b7C
b7D

[redacted]



b6
b7C
b7D

Signed by:

Click here to sign this section

Signed by [redacted] View details
on Thursday, June 16, 2011 3:56 PM (Eastern Standard Time).

b6
b7C

Signed by [redacted] View details
on Wednesday, June 22, 2011 10:11 AM (Eastern Standard Time)

FD-1023 (07/24/2010)	FEDERAL BUREAU OF INVESTIGATION

(Rev. 05-01-2008)

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 03/08/2012

To: Tampa

From: Tampa
Squad 8/Cyber
Contact: SA [redacted]

b6
b7C

Approved By: [redacted]

Drafted By: [redacted] :arm

Case ID #: 288A-TP-73999 (Pending) -22

Title: LULZSEC - SUBJECT
COMPUTER INTRUSION - CRIMINAL

INDEX
INITIALS

Synopsis: Close case.

Details: Case was initiated in order to support tasking and operation of CHS and to identify subjects in computer intrusions. CHS was very productive and information provided was used in many other FBI investigations.

No further need exists to operate CHS against LULZSEC. Writer requests to close captioned invetigation.

♦♦

UNCLASSIFIED

Close Captioned matter 8

0308 ARM 02. ec

Cat/Num Barcode	Office and Storage Location	Type	Acquired/ Chrged Out	Charged Out To/ Reason	Contributor/ Description

NO COLLECTED ITEMS FOUND FOR SELECTED REPORT